



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

**Trusted Computing Exemplar:
Personnel Security Plan**
by

Paul C. Clark, Cynthia E. Irvine, and Thuy D. Nguyen

12 December 2014

Approved for public release; distribution is unlimited

Prepared for: United States Navy, OPNAV N2/N6

THIS PAGE INTENTIONALLY LEFT BLANK

**NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000**

Ronald A. Route
President

Douglas A. Hensler
Provost

The report entitled "Trusted Computing Exemplar: Personnel Security Plan" was prepared for United States Navy, OPNAV N2/N6 and funded in part by United States Navy, OPNAV N2/N6.

Further distribution of all or part of this report is authorized.

This report was prepared by:

Paul C. Clark
Research Associate

Cynthia E. Irvine
Distinguished Professor

Thuy D. Nguyen
Research Associate

Reviewed by:

Cynthia E. Irvine, Chair
Cyber Academic Group

Released by:

Jeffrey D. Paduan
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		<i>Form Approved OMB No. 0704-0188</i>	
<p>Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>			
1. REPORT DATE (DD-MM-YYYY) 12-12-2014	2. REPORT TYPE Technical Report	3. DATES COVERED (From-To) Nov 2013 to Nov 2014	
4. TITLE AND SUBTITLE Trusted Computing Exemplar: Personnel Security Plan		5a. CONTRACT NUMBER	
		5b. GRANT NUMBER	
		5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Paul C. Clark, Cynthia E. Irvine, and Thuy D. Nguyen		5d. PROJECT NUMBER W4C05	
		5e. TASK NUMBER	
		5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER NPS-CAG-14-005	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Rhonda Onianwa OPNAV, N2/N6 F13 rhonda.onianwa@navy.mil		10. SPONSOR/MONITOR'S ACRONYM(S)	
LT David Rivera OPNAV, N2/N6F1 david.j.rivera4@navy.mil		11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			
13. SUPPLEMENTARY NOTES The view expressed in this report are those of the authors and do not reflect the official policy or position of the Department of Defense of the U.S. Government.			
14. ABSTRACT This document describes the Life Cycle Management Plan for the development of a high assurance secure product. A high assurance product is one for which its users have a high level of confidence that its security policies will be enforced continuously and correctly. Such products are constructed so that they can be analyzed for these characteristics. Lifecycle activities ensure that the product reflects the intent to ensure that the product is trustworthy and that vigorous efforts have been made to ensure the absence of unspecified functionality, whether accidental or intentional. The purpose of this plan is to provide the personnel policy necessary to protect the confidentiality and integrity of a product during the development and maintenance phases of its life cycle. Integrity is the primary concern of this plan, though confidentiality is not disregarded.			
15. SUBJECT TERMS Machinery control systems, MCS, life cycle security, high assurance, system security, trustworthy systems			
16. SECURITY CLASSIFICATION OF:		17. LIMITATION OF ABSTRACT	
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	18. NUMBER OF PAGES UU 19
		19a. NAME OF RESPONSIBLE PERSON Cynthia E. Irvine	
		19b. TELEPHONE NUMBER (include area code) (831) 656 2461	

Standard Form 298 (Rev. 8-98)

Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK



NPS-CAG-14-005



Trusted Computing Exemplar: Personnel Security Plan

Paul C. Clark
Cynthia E. Irvine
Thuy D. Nguyen

December 2014

ATTRIBUTION REQUEST

December 2014

The Cyber Academic Group (CAG) and the Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School (NPS) wish to facilitate and encourage the development of highly robust security systems.

To further this goal, the NPS CAG and NPS CISR ask that any derivative products, code, writings, and/or other derivative materials, include an attribution for NPS CAG and NPS CISR. This is to ensure that the public has a full opportunity to direct questions about the nature and functioning of the source materials to the original creators.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the following organizations for providing support toward the development of this work: OPNAV N2/N6 F1.

The material presented here builds upon work supported in previous years by the Office of Naval Research.

A portion of the material presented here is based upon work supported by the National Science Foundation under Grant No. CNS-0430566 and CNS-0430598. This document does not necessarily reflect the views of the National Science Foundation.

Table of Contents

1	Introduction.....	1
2	Policy	1
3	Responsibilities	3
	Appendix A – Participant Agreement.....	4
	Appendix B – Authorized Users on Development Systems	5
	Appendix C – Authorized Users on CM Systems	6
	Appendix D – Audit Records	7

Table of Figures

Figure 1	Sample Participant Agreement	4
Figure 2	Sample Record of Authorized Users on Development Systems	5
Figure 3	Sample Record of Authorized Users on the CM System	6
Figure 4	Sample Audit Record	7

1 Introduction

This document has been written in support of a research project to publicly demonstrate and document how a high assurance product can be developed and distributed. A high assurance product is one for which its users have a high level of confidence that its security policies will be enforced continuously and correctly. Such products are constructed so that they can be analyzed for these characteristics. Lifecycle activities ensure that the product reflects the intent to ensure that the product is trustworthy and that vigorous efforts have been made to ensure the absence of unspecified functionality, whether accidental or intentional.

The purpose of this plan is to provide the personnel policy necessary to protect the confidentiality and integrity of a product during the development and maintenance phases of its life cycle. Integrity is the primary concern of this plan, though confidentiality is not disregarded.

2 Policy

This section defines the policy with respect to personnel security, as it applies to the TCX project.

1. Specific qualifications for participation on a project (e.g., clearances, U.S. citizenship, DoD employee, etc.) are set by the Project Manager based on the needs of the individual aspects of the project (such as the projected customer base), and not as a requirement for high assurance.
2. A new user shall be promptly trained.

A new user (viz., a new participant on a project) shall be familiarized with the security requirements of the project, and trained on the proper use of the development or CM systems, before access is given to the systems. The Project Manager shall maintain evidence of this training. Training shall consist of reading the internal documents that apply to the user's responsibilities, as determined by the Project Manager. For example, a developer may be assigned to read the following documents:

- a. Physical Security Plan
- b. Personnel Security Plan
- c. Development Standards
- d. Configuration Management Procedures

Evidence of this training shall include the new user's signature indicating that the documents have been read, that they have been understood, and that the user agrees to abide by them. (See Appendix A).

3. Refresher training shall be performed annually.

All personnel involved on a project shall have a yearly refresher of the associated security requirements. The Project Manager shall maintain evidence of this training.

4. A user shall be considered authorized to access project systems after approval has been given by the Project Manager, and after training has been completed.
5. An official list of authorized users shall be maintained.

The Project Manager shall maintain two lists of authorized users:

- a. Those authorized to access CM systems. (See Appendix C).
- b. Those authorized to access development systems. (See Appendix B).

Each list shall show the full name of the user, the login name of the user, the Discretionary Access Control (DAC) groups the user is assigned to, and the date approval was given.

6. No user shall be allowed on both lists of authorized users.

The CM systems and the development systems shall have two separate system administrators.

7. A system administrator shall not add or disable accounts without direction from the Project Manager.
8. When a user separates from a project, the Project Manager shall update the list of authorized users and direct the system administrator to disable the respective account.
9. The accounts of separated users shall be disabled promptly.

When informed by the Project Manager of a separated user, the system administrator for the respective account shall promptly disable it. Confirmation of this action shall be communicated to the Project Manager, who shall note the date on the list of authorized users.

10. If a separating user is a system administrator, then the administrative password(s) shall be changed immediately.

If a new system administrator has not been identified at the time of separation, the Project Manager shall maintain the new password until a replacement has been appointed.

11. When a user separates from a project, all evaluation evidence and other project material maintained by that user shall be turned over to the Project Manager.

12. Audits shall be performed at least quarterly.

The Project Manager is responsible for verifying that all enabled accounts of the systems are on the appropriate list of authorized users.

Evidence of these audits, and their results, shall be kept by the Project Manager. (See Appendix D).

3 Responsibilities

This section assigns responsibility for meeting the requirements of this document.

1. Project Manager

The Project Manager is responsible for selecting personnel to work on a project, and ensuring that they are properly trained. The Project Manager must maintain accurate lists of authorized users, notifying the system administrators in a timely fashion when changes have been made, and conducting regular audits of the lists.

2. System Administrators

The system administrators must follow the direction of the Project Manager by either adding or disabling user accounts upon request.

3. All Project members

All members of a project must comply with the personnel policies, as stated in this document. The whole team can help the Project Manager, especially the Configuration Item Leaders, to keep track of personnel as they leave, which can be a challenge in some environments.

Appendix A – Participant Agreement

Figure 1 shows an example of an agreement that a project member is required to sign, showing evidence of initial training and a willingness to abide by the policies set forth by the project.

<p style="text-align: center;">Participant Agreement</p> <p>I have read the following documents, as directed by the Project Manager:</p> <ul style="list-style-type: none">• _____• _____• _____• _____• _____• _____ <p>I understand the above documents and agree to abide by the policies and procedures presented therein when working on the _____ project.</p> <p>_____ Printed Name</p> <p>_____ Signature</p> <p>_____ Date</p>		
---	--	--

Figure 1 Sample Participant Agreement

Appendix B – Authorized Users on Development Systems

Figure 2 shows a sample record to keep track of authorized developers, per project.

System Configuration Overview								
System Components		Performance Metrics			Resource Utilization			
Component ID	Component Name	Uptime (hrs)	Throughput (ops/s)	Latency (ms)	Memory Usage (GB)	CPU Usage (%)	Network I/O (Mbps)	Power Consumption (W)
1	Processor A	950	1200	15	16	25	100	120
2	Processor B	940	1180	16	17	26	102	122
3	Processor C	930	1160	17	18	27	104	124
4	Processor D	920	1140	18	19	28	106	126
5	Processor E	910	1120	19	20	29	108	128
6	Processor F	900	1100	20	21	30	110	130
7	Processor G	890	1080	21	22	31	112	132
8	Processor H	880	1060	22	23	32	114	134
9	Processor I	870	1040	23	24	33	116	136
10	Processor J	860	1020	24	25	34	118	138
11	Processor K	850	1000	25	26	35	120	140
12	Processor L	840	980	26	27	36	122	142
13	Processor M	830	960	27	28	37	124	144
14	Processor N	820	940	28	29	38	126	146
15	Processor O	810	920	29	30	39	128	148
16	Processor P	800	900	30	31	40	130	150
17	Processor Q	790	880	31	32	41	132	152
18	Processor R	780	860	32	33	42	134	154
19	Processor S	770	840	33	34	43	136	156
20	Processor T	760	820	34	35	44	138	158
21	Processor U	750	800	35	36	45	140	160
22	Processor V	740	780	36	37	46	142	162
23	Processor W	730	760	37	38	47	144	164
24	Processor X	720	740	38	39	48	146	166
25	Processor Y	710	720	39	40	49	148	168
26	Processor Z	700	700	40	41	50	150	170
27	Processor AA	690	680	41	42	51	152	172
28	Processor BB	680	660	42	43	52	154	174
29	Processor CC	670	640	43	44	53	156	176
30	Processor DD	660	620	44	45	54	158	178
31	Processor EE	650	600	45	46	55	160	180
32	Processor FF	640	580	46	47	56	162	182
33	Processor GG	630	560	47	48	57	164	184
34	Processor HH	620	540	48	49	58	166	186
35	Processor II	610	520	49	50	59	168	188
36	Processor JJ	600	500	50	51	60	170	190
37	Processor KK	590	480	51	52	61	172	192
38	Processor LL	580	460	52	53	62	174	194
39	Processor MM	570	440	53	54	63	176	196
40	Processor NN	560	420	54	55	64	178	198
41	Processor OO	550	400	55	56	65	180	200
42	Processor PP	540	380	56	57	66	182	202
43	Processor QQ	530	360	57	58	67	184	204
44	Processor RR	520	340	58	59	68	186	206
45	Processor SS	510	320	59	60	69	188	208
46	Processor TT	500	300	60	61	70	190	210
47	Processor UU	490	280	61	62	71	192	212
48	Processor VV	480	260	62	63	72	194	214
49	Processor WW	470	240	63	64	73	196	216
50	Processor XX	460	220	64	65	74	198	218
51	Processor YY	450	200	65	66	75	200	220
52	Processor ZZ	440	180	66	67	76	202	222
53	Processor AA	430	160	67	68	77	204	224
54	Processor BB	420	140	68	69	78	206	226
55	Processor CC	410	120	69	70	79	208	228
56	Processor DD	400	100	70	71	80	210	230
57	Processor EE	390	80	71	72	81	212	232
58	Processor FF	380	60	72	73	82	214	234
59	Processor GG	370	40	73	74	83	216	236
60	Processor HH	360	20	74	75	84	218	238
61	Processor II	350	0	75	76	85	220	240
62	Processor JJ	340	0	76	77	86	222	242
63	Processor KK	330	0	77	78	87	224	244
64	Processor LL	320	0	78	79	88	226	246
65	Processor MM	310	0	79	80	89	228	248
66	Processor NN	300	0	80	81	90	230	250
67	Processor OO	290	0	81	82	91	232	252
68	Processor PP	280	0	82	83	92	234	254
69	Processor QQ	270	0	83	84	93	236	256
70	Processor RR	260	0	84	85	94	238	258
71	Processor SS	250	0	85	86	95	240	260
72	Processor TT	240	0	86	87	96	242	262
73	Processor UU	230	0	87	88	97	244	264
74	Processor VV	220	0	88	89	98	246	266
75	Processor WW	210	0	89	90	99	248	268
76	Processor XX	200	0	90	91	100	250	270
77	Processor YY	190	0	91	92	101	252	272
78	Processor ZZ	180	0	92	93	102	254	274
79	Processor AA	170	0	93	94	103	256	276
80	Processor BB	160	0	94	95	104	258	278
81	Processor CC	150	0	95	96	105	260	280
82	Processor DD	140	0	96	97	106	262	282
83	Processor EE	130	0	97	98	107	264	284
84	Processor FF	120	0	98	99	108	266	286
85	Processor GG	110	0	99	100	109	268	288
86	Processor HH	100	0	100	101	110	270	290
87	Processor II	90	0	101	102	111	272	292
88	Processor JJ	80	0	102	103	112	274	294
89	Processor KK	70	0	103	104	113	276	296
90	Processor LL	60	0	104	105	114	278	298
91	Processor MM	50	0	105	106	115	280	300
92	Processor NN	40	0	106	107	116	282	302
93	Processor OO	30	0	107	108	117	284	304
94	Processor PP	20	0	108	109	118	286	306
95	Processor QQ	10	0	109	110	119	288	308
96	Processor RR	0	0	110	111	120	290	310

Figure 2 Sample Record of Authorized Users on Development Systems

Appendix C – Authorized Users on CM Systems

Figure 3 shows a sample record to keep track of authorized users on the CM system.

Figure 3 Sample Record of Authorized Users on the CM System

Appendix D – Audit Records

Figure 4 shows a sample record to provide evidence that audits were performed as required.

Audit Record		
Description of item(s) under audit:		
Findings:		
Audited by:		
Printed Name	Signature	Date

Figure 4 Sample Audit Record

[THIS PAGE IS INTENTIONALLY BLANK]

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center Ft. Belvoir, Virginia	2
2. Dudley Knox Library, Code 013 Naval Postgraduate School Monterey, California 93943	2
3. Research Sponsored Programs Office, Code 41 Naval Postgraduate School Monterey, California 93943	1
4. Paul C. Clark Naval Postgraduate School Monterey, California 93943	1
5. Dr. Cynthia E. Irvine Naval Postgraduate School Monterey, California 93943	1
6. Thuy D. Nguyen Naval Postgraduate School Monterey, California 93943	1